HAL
open science

Radiated Electromagnetic Emission for Integrated Circuit Authentication

Mosabbah Mushir Ahmed, David Hely, Nicolas Barbot, Romain Siragusa, Etienne Perret, Maxime Bernier, Frédéric Garet

To cite this version:

Mosabbah Mushir Ahmed, David Hely, Nicolas Barbot, Romain Siragusa, Etienne Perret, et al.. Radiated Electromagnetic Emission for Integrated Circuit Authentication. IEEE Microwave and Wireless Components Letters, 2017, 27 (11), pp.1028 - 1030. 10.1109/LMWC.2017.2750078 . hal-01724143

HAL Id: hal-01724143

https://hal.science/hal-01724143v1

Submitted on 1 Jul 2020

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Radiated Electromagnetic Emission for Integrated Circuit Authentication

Mosabbah Mushir Ahmed, David Hely, Nicolas Barbot, Romain Siragusa, Etienne Perret, Maxime Bernier, Fredric Garet

***Abstract*—Counterfeiting of integrated circuit (IC) is a growing concern in the semiconductor industry. Counterfeiting involves economical and safety issues. Both semiconductor companies and embedded system designers are looking for traceability solution in order to get assurance in IC they use. This letter proposes to use Electromagnetic (EM) radiated emission from Integrated Circuits (IC) to create a unique fingerprint for each IC. We have proposed to use a variability-aware circuit configuration which would exploit EM fingerprint for each IC. Our measurement results on two different field-programmable gate array (FPGA) families over several test boards validates this scheme. As a last step, post-processing on the obtained EM measurements is done to get a unique FPGA signature which could be used for the purpose of authentication.**

Keywords*—*Electromagnetic Emission, Integrated Circuit, Authentication

I. Introduction

In recent years there has been a growing number of incidents of IC counterfeiting [1]. There are primarily two methods to address IC counterfeiting. The first method is based on counterfeit detection using classical electrical and physical methods. From [1], this method is very invasive, time-consuming and involves the risk of damaging the IC. The second method is based on the traceability approach to find a unique signature for authentication by using process variations (PV). Based on PV, Physical Unclonable Function (PUF) approach is mostly used. In [2], a PUF is based on the idea that each IC is different due to the normal manufacturing variability even though they are from the same manufacturing mask. A PUF uses an input challenge c, and returns a response r. Each c-r pair is unique. A PUF requires dedicated on-chip circuitry for the post processing of the PUF response, which may be complex to process and implement.

We propose a method of authenticating an IC using an EM based approach. Thanks to the PV from an IC, each IC has a unique EM signature that can be used as its fingerprint for authentication. This work first focuses on FPGA, which is a common target of counterfeiting. Our method targets to authenticate new FPGAs to prevent theft or counterfeit during the supply from original component maker (OCM) to the customer. We have implemented a variability-aware circuit in FPGA and attempted to obtain a unique signature for authentication for each FPGA due to the effect of PV on the variability-aware circuit. Compared to the existing methods (electrical and physical) to detect counterfeit IC our method is close to being non-intrusive, requires less time and involves no risk of damaging the IC. In comparison to the PUF approach, our methodology uses less silicon area. The main difference is that for PUF the processing is done on-chip (inside the IC) whereas in this methodology it is done outside the IC. This is an advantage in terms of design cost. As a potential limitation, the IC cannot use the authentication information.

FPGAs are powerful devices in terms of flexibility and programmability. It has been shown in [3] that a periodic oscillating RF signal can even be generated inside that component. The signal frequency can be higher (upto 500 MHz) than the ones typically used for classical operations. One way to detect this RF signal is to use a magnetic probe placed just above the FPGA. The idea here is to see that the RF signal produced by the FPGA can be used for authentication purpose in the RF domain. Indeed, ring oscillator (RO) circuit is a variability-aware circuit because the oscillating signal frequency it generates, is sensitive to the manufacturing induced PV in IC. It is one of the commonly used oscillator circuit in RF applications and has the advantages of power efficiency, low area occupancy of chip and rail to rail voltage swing [4]. The oscillation of RO circuit depends upon switching speed of the transistors of inverter.

II. Authentication Methodology and Effects of PV on RO

The proposed methodology for authentication is illustrated in Fig. 1. The methodology is divided broadly into a few steps: creating a fingerprint by doing a set of measurements, storing the fingerprints in database and performing the same measurement and comparing the values from database in order to authenticate the IC. Two main conditions must be satisfied

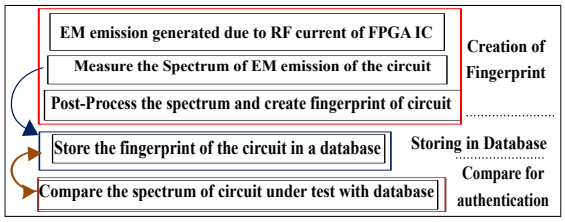

Fig. 1: Proposed methodology for authentication using radiated EM approach

in order to support the validity of using EM signature for authentication purpose : first, the signature has to vary between different ICs, second for the same IC the signature has to be constant over time. To find a degree of similarity between response from two ICs, we have used Cosine Similarity (CS) as a post-processing tool. CS gives a score based on the similarity

This work was supported in part by the University of Grenoble Alpes and the Région Auvergne-Rhône-Alpes via the ARC6 program. M.M.Ahmed, D. Hely, N. Barbot, R. Siragusa and E. Perret are with the LCIS - Grenoble Institute of Technology, Valence, France (e-mail: mushir-mosabbah.ahmed@lcis.grenoble-inp.fr). E. Perret is also with the Institut Universitaire de France, Paris, France. M. Bernier and F. Garet are with the IMEP-LAHC - University of Savoie Mont Blanc, Chambery, France.

of two vectors. Higher score means more similarity between the dataset [5].

The variability due to PV in ICs is a unique and a random phenomenon which gives unique physical features to ICs even if they are from the same lithographic mask [6]. In this work, the implemented RO circuit exploits spatial form of variability. As also discussed in [6], the spatial variability comes due to manufacturing errors like random dopant fluctuations (RDF), lithographic errors, geometric variation in transistors and interconnects etc. which affects the V_{th} (threshold voltage) and output capacitances of the RO circuit transistors. The voltage V_{th} and output capacitances affects the switching speed and propagation delay of the transistors of each inverter of RO circuit [7].

III. Ring Oscillators Description

The RO typically consists of an odd number of inverters (delay elements) in a cycle. The last stage of the RO is connected to the first stage as a feedback which causes a sustained oscillation by the circuit. For a sustained oscillation, the ring must provide a phase shift of 2π, where each inverter stage provides a phase shift of π/n (where n is number of inverters), the another π phase shift comes from DC inversion and the gain at frequency of operation should be unity [4]. A single inverter with the feedback does not provided enough phase shift for a sustained oscillation, because of which RO must have minimum of three inverters. From [7], the variation in frequency of oscillation in RO is related to device parameters like transistor switching speed and the capacitive load of the next step. In this work, a three inverter stage RO with an AND gate is used as shown in Fig. 2. The purpose of AND gate is only to enable (using EN pin) the logic. The equation

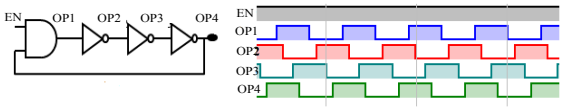

Fig. 2: Three Stage Ring Oscillator. (a) Circuit Diagram of 3-stage RO. (b) Timing diagram of 3-stage RO.

for frequency of the RO circuit considering the delay due to inverter and AND gate, can be given by

$$f_n = 1/(2 * (n * t_d + \tau)) \tag{1}$$

where
n is the number of inverters.
t_d is the propagation delay due to a single inverter.
τ is the delay due to the AND gate.

From (1), it is clear that the number of inverters is inversely proportional to RO frequency which is also shown in the Fig. 3. The spectral response in a bandwidth ranging between 100 MHz and 800 MHz, for three different configurations of RO circuit is shown in the Fig. 3. In this bandwidth range, the spectrum of RO fundamental frequency, the first harmonic and the second harmonic are depicted in Fig. 3. As the order of harmonic increases, the magnitude of signal decreases which is also clear from Fig. 3. In this work, we have used only the fundamental frequency of the RO circuit.

IV. Measurement and Results

Fig. 4 illustrates the measurement setup. To extract the EM emission from the FPGA, a H-field near field RF-U 5-

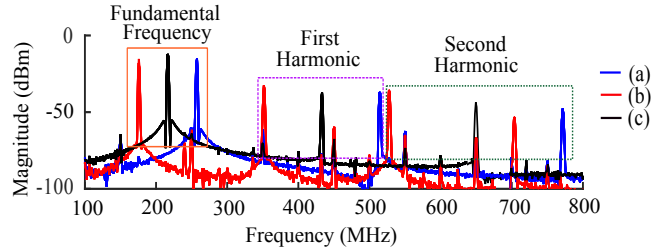

Fig. 3: Frequency of RO for varying interconnect lengths and no. of stages of inverter (showing fundamental frequency as well as the higher harmonics). (a) A 3-stage inverters RO (b) A 5-stage inverter RO (c) A 3-stage inverters RO with longer interconnect length between logic elements.

2 probe from Langer EMV Technik GmbH is used. In our measurements, two different families (technologies) of FPGAs are considered: ARTIX-7 (28 nm) and SPARTAN-3E (90 nm). From [6], as the CMOS scales down sub 90 nm technology, the effect of PV is more noticeable. Our aim is to observe the effects of PV on RO in two different families of FPGA and determine which gives a higher degree of uniqueness in the fingerprints. Frequency of RO circuit in two families differs because of the difference in switching speed of transistor (28 nm FPGA would switch faster), internal routing structure of each family and other layout difference in the IC. A single RO circuit is placed at the center of FPGA and the probe is moved over several positions. The near field probe is moved in 2D X & Y directions, to find the spot over FPGA where the signal to noise ratio (SNR) of EM emission due to the RO is maximum. The magnetic field probe is oriented horizontally to measure the field emitted vertically from the IC. Measurements are repeated 15 times to see the robustness of the result. The spectrum range is observed upto 2 GHz with 64 points averaging.

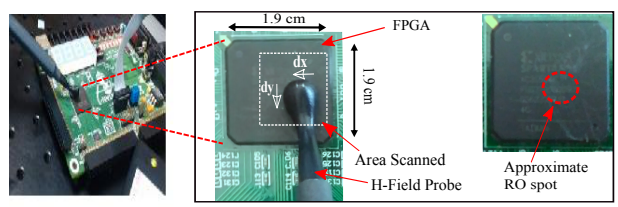

Fig. 4: Measurement setup: FPGA board with probe. The insert zoom shows the area scanned by H-field probe in X-Y direction where dx=dy=1mm is the unit distance and approximate spot where RO circuit is placed in the FPGA

A. ARTIX-7 Results

As seen from (1),3-stage RO gives maximum frequency of oscillation, taking this into consideration we have implemented a 3-stage RO in the FPGA. The same 3-stage RO has been implemented on 4 different ARTIX-7 FPGAs. Each has been measured 15 times with the setup shown in Fig. 4, following the same experimental protocol. Each device under test (DUT) has been removed and repositioned between each measurement in order to take into account the systematic errors. The repeated spectral responses are depicted in Fig. 5 over a bandwidth spreading from 300 MHz to 800 MHz. In this bandwidth range first harmonics are observed along the fundamental frequencies of each DUTs. The values from TABLE I and spectral response from Fig. 5 shows a unique frequency for different FPGA having same RO circuit.

To find a degree of similarity, Cosine Similarity (CS) is performed as post-processing part on the obtained signals from 4 DUTs. The CS is performed on complex part of the signal

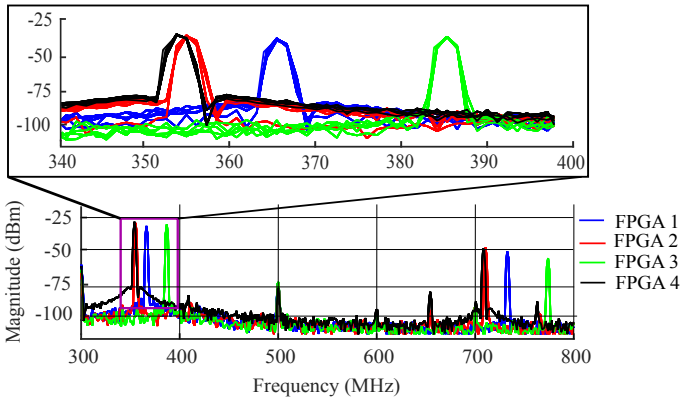

Fig. 5: RF signals emitted 4 different ARTIX-7 FPGAs with same RO circuit, range upto 800 MHz shows first harmonics and (insert) a zoom in around the fundamental frequency peak (exhibiting the repetitive measurements).

which also uses phase information of the signal. From now on, we use the terms auto-correlation (AC) and cross-correlation (CC), to refer to the CS computed from two measurements performed on a single DUT, and computed from two different DUTs, respectively. The total combinations obtained for AC is 420 and for CC is 1350 from 15 measurements on 4 DUTs. CS is performed in two spectral ranges: *a)* entire range (0 to 2 GHz) of spectrum , *b)* in the particular range of fundamental frequency (approximately in the window of ≈ 5 MHz centered around fundamental frequency). In both the cases, results of CS are comparable. The observed CS scores is, worst case CC≈ 0.16 and AC≈ 0.82 for each measurement of all 4 DUTs. Fig. 6(a) shows the CS score distribution of all 4 DUTs, where $da(\approx 0.64)$ indicates the difference between worst case of AC and CC scores. Even though the spectrum of DUT 2 and 4 are closer but the CS computation gives CC score under ≈ 0.16, this is because of high Quality factor (Q-factor) of the signal. This determines that even the statistical overlapping of the AC and CC values is not forbidden, but due to the high Q-factor of the obtained EM signals from the FPGAs, the overlap in AC and CC values is null in all our measurements. Hence a single frequency of resonance to compute or extract a unique fingerprint is sufficient if the Q-factor of signal is high. Based on the results from Fig. 5, TABLE I, and the CS score distribution in Fig. 6(a), we can conclude that each FPGA has a unique EM emission due to effect of PV on RO circuit which can be used for authentication.

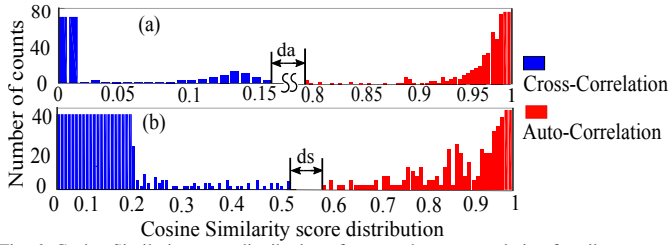

Fig. 6: Cosine Similarity score distribution of auto and cross-correlation for all measurements of a) ARTIX-7, and b) SPARTAN-3E FPGA.

B. Results of SPARTAN-3E

The same 3-stage RO has been implemented on 8 different SPARTAN-3E FPGAs. The spectral responses are depicted in the Fig. 7 over a bandwidth spreading from 100 MHz to 530 MHz, shows first harmonic along the fundamental frequencies of each 8 DUTs. TABLE I shows the unique frequency values of each FPGA. Similar post-processing steps are performed as

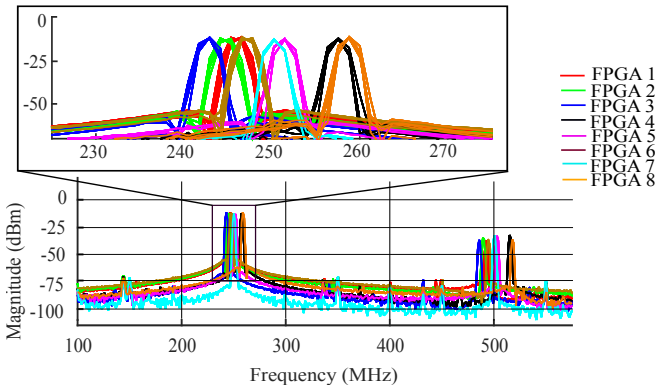

Fig. 7: RF signals emitted by 8 different SPARTAN-3E FPGAs with the same RO circuit, range upto 530 MHz. and (insert) a zoom in around the first oscillation peak(with repetitive measurements)for all DUTs.

done in ARTIX-7 case. The total combinations of AC is 840 and CC is 6300 for 15 measurements on 8 DUTs.

The results obtained for the CS score is, worst case score for AC≈ 0.5 and CC≈ 0.6. Fig. 6(b) shows the CS score distribution of all 8 DUTs, where $ds(\approx 0.1)$ indicates the difference between worst case of AC and CC scores.

TABLE I: Mean Frequency (MHz) of RO of 4 and 8 FUTs of both families

FPGA	1	2	3	4	5	6	7	8
ARTIX -7	366.2	355.2	387	354	-	-	-	-
SPARTAN -3E	246.6	245.4	242.9	257.6	251.5	247.8	250.2	258.8

V. Conclusion and Future Work

In this letter we proposed a method to quantify EM emission from RO circuit, that can be implemented to create a unique signature of FPGA. The proposed technique is cost and time effective, easy to implement and non-invasive. The score distribution of AC and CC, show that this methodology can be effectively implemented to authenticate FPGA. Similar approach can be applied as part of future work to authenticate ASIC. On-going work aims at evaluating the aging effect on FPGAs for authentication and proposing solution to increase the robustness of the existing method.

References

[1] Kai He, Xin Huang and Sheldon X.-D Tan,"EM Based on-Chip Aging Sensor for Detection and Prevention of Counterfeit and Recycled ICs" *IEEE/ACM Int. Conf. on Computer-Aided Design (ICCAD)*, Austin, TX, 2015, pp. 146-151.

[2] Charles Herder, Meng-Day (Mandel) Yu, Farinaz Koushanfar, and Srinivas Devadas, "Physical Unclonable Functions and Applications: A Tutorial" in *Proc. of IEEE*, vol. 102, no. 8, 2014, pp. 1126-1141.

[3] Franco Fiori and Francesco Musolino "Comparison of IC Conducted Emission Measurement Methods" in *IEEE Trans. Instrum. Meas*, vol. 32, no. 3, 2003, pp. 839 - 845.

[4] S. Docking and M. Sachdev, "A method to derive an equation for the oscillation frequency of a ring oscillator," in *IEEE Trans. Circuits Syst. I, Fundam. Theory*, vol. 50, no. 2, 2003, pp. 259-264.

[5] Chouchang Yang, Alanson P. Sample, "EM-ID: Tag-less Identification of Electrical Devices via Electromagnetic Emission" *2016 IEEE Int. Conf. on RFID (RFID)*, Orlando, FL, 2016, pp. 1-8.

[6] Swaroop Ghosh and Kaushik Roy, "Parameter Variation Tolerance and Error Resiliency: New Design Paradigm for the Nanoscale Era", *in Proc. of the IEEE*, vol. 98, no. 10, 2010, pp. 1718-1751.

[7] Borivoje Nikolić, Bastien Giraud, Zheng Guo "Technology variability from a design perspective" in *IEEE Trans. Circuits Syst. I, Fundam. Theory: Regular Papers*, vol. 58, no. 9, 2011, pp. 1996-2009.